7 November 1979

MEMORANDUM FOR MEMBERSHIP OF COMPUTER SECURITY SUBCOMMITTEE, SECOM, NFIB

SUBJECT: Security Considerations Existing/Developing in Word Processing or Automated Office Systems -- INFORMATION MEMORANDUM

1. The last five years have seen an amazing and steadily accelerating growth throughout the Federal Government and U.S. industry of both stand-alone and computer-associated word processing or automated office systems. Because of their low cost, smaller size, potential telecommunications capabilities (electronic mail) and data processing capabilities, increasing numbers, and frequent use outside normal data processing environments, these automated mini/micro systems often present special security problems.

2. The purpose of this memorandum is to alert members of the Intelligence Community to the existence of a family of security vulnerabilities now extant, and growing daily, in potential danger of exploitation by hostile intelligence services targeted against U.S. facilities abroad and within the American continent.

3. Because the vulnerabilities of most automated systems tend to increase hand-in-hand with their multiplying complexity, it might be well for management purposes to categorize the word processing systems into two types:

a. Independent or Stand-alone Systems. Defined as individual word processing stations or devices, operating independently, dedicated to one operator. These stations do not share memory or magnetic storage media with other stations or devices and are not capable of communicating with any other peripheral device or equipment.

b. Resource-sharing and Communicating Systems. Defined as processing systems which have a computer, mini-computer, or microprocessor as an integral part of the system. These are true automated systems, as contrasted with the independent station, which is really an automatic typewriter. The computer-centered systems share a single CPU, memory, and magnetic storage media. The more sophisticated models also include the capability of intercommunication with other remotely located units, either via their own CPU or via another common-user network, a capability commonly referred to as "electronic mail."

4. Each word processing or automated office system must be evaluated, security-wise, on an independent basis--individual characteristics must be taken into account. The independent or stand-alone word processing (WP) station with volatile buffers and memory, small removable magnetic storage media (i.e., floppy disk), and good TEMPEST characteristics (minimal text-bearing spurious electromagnetic radiation) would appear to require the least risk analysis and provide most acceptable security. On the other hand, the more complex systems, incorporating shared memory and storage, internal system communication or external telecommunications capabilities (electronic mail/automated office systems), are going to require a total systems security approach to their risk analysis and management in their evaluation and formal accreditation by responsible managers or commanders. Some factors which will have bearing in the risk analysis of these shared-resource systems are:

a. Removable or fixed magnetic media (some stand-alone WP having fixed-disk memory/storage constitute unacceptable security risk for classified processing unless employed in a controlled area).

b. Whether system has volatile or non-volatile buffers and/or memory. If non-volatile, are proven and acceptable "clear buffer memory" routines available and used? Can full erasure be verified?

c. What methods are used to degauss all disk packs or other magnetic media prior to release to vendor or re-utilization outside classified media control?

d. What methods and/or containers are employed to protect software and data stored on magnetic media?

e. If WP is employed in forward areas or areas in which they might be overrun or seized by terrorist groups, is provision made for the emergency destruction of sensitive data?

f. If the system features electronic mail/automated office capabilities, what COMSEC/EMSEC measures are employed?

g. Is the resource-shared word processing system dedicated exclusively to text manipulation and storage functions, or is it connected to a computer employed on command/control, intelligence, management information, or business applications?

h. Does system have audit trail and security officers who monitor entry and file access?

i. Level of classification for each network node; security consideration posed.

j. System access and authorization.

5. Answers to the questions posed above will enable a security-knowledgeable individual to begin an approach toward analyzing and managing the risks to security which an automated word processing system poses. A full-fledged analysis, required by Transmittal Memorandum #1 to OMB Circular 71 for system accreditation, will, of course, necessitate a broader examination of all of the impacts of the eight automation security subdisciplines--physical, personnel, hardware, software, procedural, communications, emanations, and educational.

Prepared by:
CSS Working Gp on WP

STAT